DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
2531 JEFFERSON DAVIS HWY
ARLINGTON VA 22242-5160

IN REPLY REFER TO

5239
SER00I/P12
15 APR 02

**POLICY LETTER 12-02**

From: Naval Sea Systems Command, Chief Information Officer (SEA 00I)

Subj: NAVSEA ENTERPRISE POLICY ON PORTABLE ELECTRONIC DEVICES (PEDs)

Ref: (a) CNO Message, 272200Z APR 01, POLICY UPDATE: USE OF PORTABLE ELECTRONIC DEVICES IN THE NAVY

(b) NAVSEA ENTERPRISE-WIDE PERSONAL DIGITAL ASSISTANT (PDA) AND WIRELESS PAGER/EMAIL DEVICE POLICY, Ser 00I/123, 15 May 2001

(c) National Security Agency (NSA) Information Assurance Advisory No. IAA-001-01, "Personal Electronic Devices Security Guidance," 16 January 2001

(d) Naval Computer Incident Response Team (NAVCIRT) Advisory 00-028, 131301Z JUL 00, PERSONAL DIGITAL ASSISTANTS (PDA) SECURITY CONSIDERATIONS

(e) DoD 8510.1-M, 31 July 2000, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual

(f) COMNAVNETOPSCOM INSTRUCTION 5400.1, "Navy and Marine Corps Intranet (NMCI) Personal Digital Assistants (PDA)/Wireless Policy," 29 January 2002

Encl: (1) PED Vulnerabilities and Risks

1. Purpose: This memorandum disseminates policy and guidance for the acquisition and use of wireless communication solutions and PEDs, including data-enabled cellular phones, two-way pagers, personal digital assistants (PDAs), and handheld/laptop computers. Reference (a) prescribes high-level PED policy for the entire Navy and invites the Cognizant Security Authorities to provide more detailed and specific policies for PEDs, based upon operational risk assessments and available countermeasures. This PED policy and Reference (f) include guidance for PDAs; therefore, this policy replaces Reference (b).

2. Scope: This policy applies to NAVSEA Headquarters and the NAVSEA field activities. All NAVSEA personnel, including contractors working for NAVSEA, shall adhere to the provisions of this policy. PEDs covered by this policy include, but are not limited to, the following:

a. Mobile computing devices (e.g. Personal Digital Assistants, handheld PCs, notebook PCs)

b. Mobile Telephony Devices

c. Pagers, including those with e-mail capabilities (e.g. Blackberry)

d. Digital Cameras (Still and Video)

e. Analog and Digital Sound Recorders

This policy also applies to all forms of removable storage media such as flash memory, memory "sticks", Multimedia Cards & Secure Digital Cards, micro-drive modules, ZIP drives, ZIP disks, recordable CDs, DVDs, and floppy diskettes.

3. Discussion: PEDs and wireless technologies present a significant security risk when operated outside of guidelines. Backdoors into NAVSEA Local Area Networks (LANs) could be caused by either unprotected transmissions or unprotected PEDs entering the network. Encl. (1) summarizes the vulnerabilities and risks outlined in References (c) and (d). NAVSEA intends to minimize the risk of inadvertent loss or compromise of classified or sensitive U.S. Government information due to the introduction of PEDs into NAVSEA work environments. NAVSEA also intends to thwart deliberate damage to, or compromise of, its information systems and networks resulting from exploitation of PED capabilities. Therefore, this policy is intended to fully inform NAVSEA employees of:

a. The vulnerabilities and risks posed by the presence of PEDs in areas where classified or sensitive information and information systems are located.

b. The need to provide proper security awareness training to each user being issued a PED regarding the physical and information security vulnerabilities of the device.

c. The need for PED solutions that are engineered to preclude backdoors into the NAVSEA LANs.

4. Policy: The use of PEDs in NAVSEA work environments shall be in accordance with the following:

a. PEDs that are synchronized with desktop computers on NAVSEA networks shall adopt the following security measures:

(1) PEDs will not be connected to systems or networks processing NAVSEA information without cognizant DAA approval.

(2) PEDs will only synchronize with unclassified computers.

(3) PED wireless connectivity features shall not be active while the PED is physically connected to a desktop PC or otherwise connected to the network.

b. No PEDs shall be brought into a Sensitive Compartmented Information Facility (SCIF), except where specifically authorized in writing by the cognizant Designated Approving Authority (DAA). Such authorization shall include the requirement to disable the infrared (IR) and radio frequency (RF) capabilities of the PED before it is brought into the SCIF.

c. Personally owned PEDs (except for voice-only cellular telephones) are not authorized for use at any NAVSEA facility unless specifically authorized in writing by the cognizant DAA. This is to minimize the risk of inadvertent capture of controlled information by a personal PED, since the only approved method of "sanitizing" most PEDs is physical destruction.

d. PEDs will not be used to store passwords, safe nor door combinations, personal identification numbers (PINs) nor classified information.

e. With the exception of approved laptop computers, PEDs will not be used for processing Naval Nuclear Propulsion Information (NNPI).

f. All wireless communication systems must be certified and accredited in accordance with Reference (e). Pilot projects must implement appropriate security requirements and processes during the development of the system.

g. PEDs shall be configured with appropriate security settings prior to being issued to users. Passwords shall be a minimum of eight alphanumeric characters. PED

devices shall be set to require password re-authentication after a maximum of thirty minutes of inactivity.

h. PEDs shall not be used for classified information processing unless specifically authorized in writing by the cognizant DAA.

i. *PEDs without Identification & Authentication capabilities* built-in or added to the system shall be used only for administrative tasks, such as maintaining appointment calendars and non-sensitive contact lists.

j. Where feasible, PEDs shall employ up-to-date signature files that are used to profile and identify viruses, worms, and malicious code. As proven anti-virus clients for PEDs become available, these clients shall be deployed to the greatest possible extent in all PEDs that connect to the network.

k. Personal Area Networks (e.g., Bluetooth) have well-documented vulnerabilities that are easily exploited and are prohibited from processing NAVSEA information. Security features of these products are either non-existent or too immature to be safely deployed in the near future.

l. Web-enabled PEDs that rely on Wireless Access Protocol (WAP) and/or use commercial wireless service providers shall not be used for processing sensitive or controlled information unless it can be shown that the data is encrypted end-to-end using a FIPS 140-1 or 140-2, Level 1 (or higher) approved cryptomodule.

5. Responsibilities:

a. Commanding Officers/DAAs shall:

(1) Ensure that PED use under their purview is in accordance with this policy.

(2) Develop appropriate and effective procedures for local implementation of this policy.

(3) Ensure that the local ISSM/ISSOs are familiar with References (c) and (d).

b. The NAVSEA DCIO for Operations shall:

(1) Ensure that all PEDs issued at HQS are properly configured prior to their issuance to users.

c. The NAVSEA DCIO for Information Assurance shall:

(1) Develop and present appropriate security awareness training as required for PED users at NAVSEA HQS.
(2) Maintain this policy.

d. Program Managers of PED solutions shall:

(1) Implement this policy as applicable in their programs, to include careful consideration of the vulnerabilities and risks associated with the design of wireless solutions.

(2) Upgrade or replace PEDs that do not comply with this policy.

6. The marketplace for PEDs is very dynamic and rapidly evolving as wireless technologies continue to proliferate at rapid rates. It will be necessary to update and refine this policy as newer and more capable products become available. Moreover, Reference (f) contains Navy policy and specific security guidance for use of PDAs and other emerging wireless solutions in NMCI. This NAVSEA PED policy is consistent with the NMCI policy and will be reviewed on a regular basis to ensure that future versions of this policy will be harmonized with NMCI products and policies as appropriate.

7. In the event you experience an adverse impact on business operations as a result of this policy, please bring it to my attention. If you have any other questions or concerns, please contact Mr. Tony Geddie, Deputy CIO for Information Assurance at (202) 781-3014 or GeddieJA@navsea.navy.mil.

S. J. BOURBEAU
CHIEF INFORMATION OFFICER
NAVAL SEA SYSTEMS COMMAND

15 April 2002

## PED Vulnerabilities and Risks

This Enclosure summarizes the contents of NAVCIRT Advisory 00-028 and NSA Information Assurance Advisory IAA-001-01. It is intended as a quick reference guide of essential precautions for using Portable Electronic Devices (PEDs) to process classified and controlled unclassified information in sensitive areas. Reading this Enclosure is not a substitute for reading the references themselves.

**Introduction.** The capabilities of PEDs, and their use in areas where sensitive or classified information may be discussed, stored, or processed, create higher levels of security risk. Therefore, use of such devices must be carefully managed.

**Sources of Risk.** Built-in PED features, such as infrared, radio frequency, and telephone modem communications capabilities, create new attack avenues that can be easily exploited by knowledgeable adversaries. These features are difficult to disable effectively when situations call for these capabilities to be temporarily deactivated. Some of the highest risk features are:

(1) infrared (IR) communications capability - can send and receive data without indication to the user; moreover, covering the IR port with an opaque covering is often not effective.

(2) wireless RF communications capability - also can send/receive data without indication to the user, at LAN speeds or medium-speed cell phone rates; removal of the antenna does not eliminate the risk.

(3) external device (modem, IR hub, IR scanner, PDA sync cradle) connectivity - must never be left unattended, as they create covert connection paths that are easily exploited to install undesirable code or deliver bogus data without the user's permission. These types of connections can also be exploited to install "back doors" to an otherwise secure host network, especially when combined with "Trojan horse" code.

(4) untrusted software upgrades/enhancements - these are easy to use and easy to exploit for installing Trojan horse code or other types of malicious code without the user's knowledge or consent. Malicious code is known to be distributed via freeware and shareware channels, especially in games and entertainment software. In addition to activating "back doors" to host networks, this code can also e-mail the user's information and personal data to a hacker's account, and/or exploit wireless connections that may be available on the user's PED.

(5) removable peripheral/expansion devices - these devices, such as PC cards or "smart" cards, often have independent processing capability. Having a PED designed to accept such devices makes it easy to substitute a physically identical device containing malicious functionality.

(6) removable storage media - flash memory cards, memory "sticks," microdrive modules, floppy diskettes, and similar storage devices containing sensitive or classified data can be easily lost or stolen if left unattended.

(7) remote viewing of PED display screens - techniques exist by which electronic display screens can be viewed with surprising accuracy from much greater than expected distances.

(8) audio and video recording capabilities and devices - the vulnerabilities and risks of using these devices in sensitive areas are obvious.

**Physical Security of PEDs.** The continuous physical security of PEDs is of paramount importance, especially if they are routinely allowed into secure spaces. PEDs contain all of the components needed for a sophisticated, remotely activated surveillance device, and can be reconfigured as such in 30 minutes. Users must protect their PEDs assiduously during transit, continuously observe the PEDs when they are connected to an Ethernet cradle or other device that furnishes access to a network, and report any suspicious activity involving their PEDs to their security office.

**Dos and Don'ts for PED Usage.** The following guidelines are the minimum essential for secure use of PEDs throughout NAVSEA:

(1) Use in PEDs only commercial shrink-wrapped software from trusted sources. Exceptions to this rule must be approved by the cognizant DAA.

(2) Connect PEDs to UNCLASSIFIED computers only.

(3) Never store passwords, combinations, PINs nor classified information in a PED.

(4) Disable the wireless capabilities of the PED, if any, when it is connected to a desktop PC or any other device connected to a network.

(5) Never use PED wireless features, inside a Sensitive Compartmented Information Facility (SCIF).

(6) At a minimum, PEDs shall be turned off when carried into secure spaces where classified information exists.

**Special Precautions for Classified PEDs.** Classified use of PEDs must be expressly authorized by the cognizant DAA. Unless an exception is specifically authorized in writing by the cognizant DAA, the following precautions must be observed when using PEDs in classified information environments:

(1) A PED containing classified information must be controlled in the same manner as material of the same or higher classification. For this reason, classified PEDs must be given distinctive external labels that clearly state the highest classification of information they contain.

(2) Never connect a classified PED to a computer network, nor to stand-alone computers of lower (or higher) classification.

(3) Never exchange data between a classified PED and an unclassified PED.

(4) Never use wireless modems with classified PEDs.

(5) Classified PEDs cannot be declassified by any method other than physical destruction. A "hard reset" cannot declassify a classified PED. Accordingly, the decision to load classified information into a PED must be made thoughtfully with full awareness of the consequences.